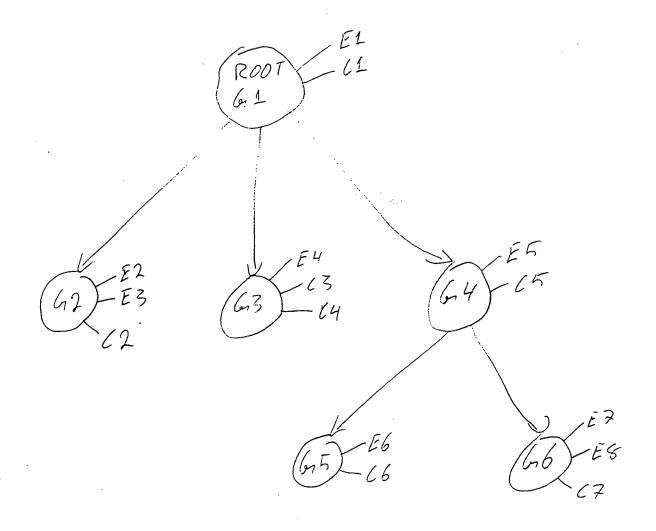


FTG. 1

(MIN)
RECEIVE REQUEST FOR TICKET
DE LECENTER HU
REGISTERED MU
1,789
ACCESS DATA BASE 230
LOCATE GROUP IN DATABAGE
AND ALL AMCESTOR GEOUPS 240
LONGTRUCT SUMMARY OF
EVENTS ASSOCIATED W
CLIENT BY ADDING IDENTIFYING
INFO FOR EACH EVENT IN
THE GIZOUP AND ANCESTOICS 250
TRANSMIT TICKET TO
(LIENT 260 (EMI)

EG. 2.

## ASSOCIFTIUE DATABLE



FJ61.3

410 GROUP IDENTIFIER

EVENT1 - TITLE 421, IP \*DRESS OF

SENDING CLIENT 422, TIME

INDICATION 423, IP \*ADDRESS

OF KEY SERVER 424.

EVENT 2

EVENT M

430 DIGITAL CERTIFICATE

FIG. 4

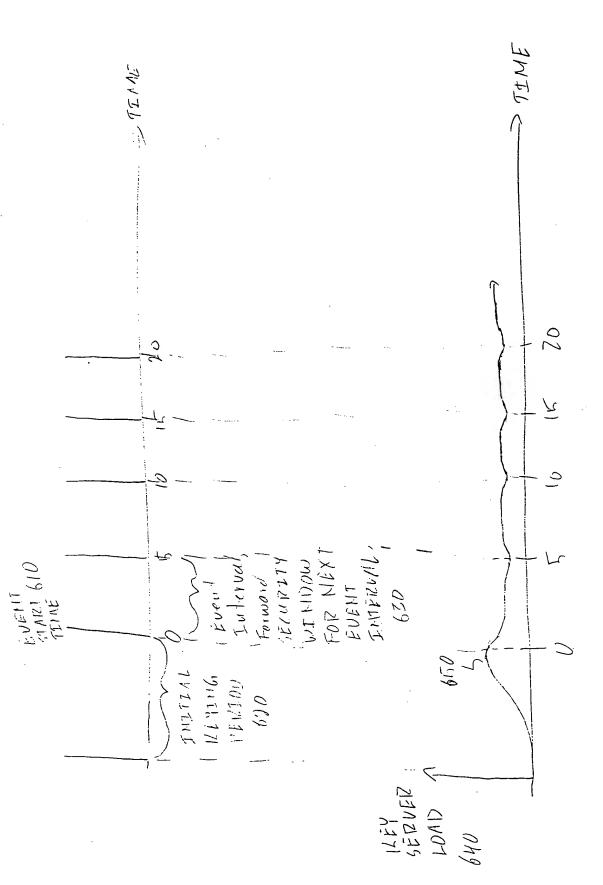
530

(BEO. M)
(1960-17)

509 RECEIVE INITIAL REQUEST FOR KEY AT A RANDOMLY GENERATED TIME DURING KNOWH PERIOD REFORE THE EVENT PREDETERMINED ESTABLISH POINT-TO-POINT LINK BETWEEN 510 KEY GERVER AND CLIENT 515 CREDENTIALS FROM TICKET UERIFY KEY, INCLUDING TRANSMIT INITERL SYMMETRIC CRYPOGRAPHIC ILEY, INITIATION GENDER) LND TEME (SYNCHRONITED FOR 520 LEY LIFETIME 525 REFRESH REQUEST AT A RECEIVE RANDOMLY GENERATED PARTICULAR TIME INTERVAL BASED ON A FORWARD SECURITY WINDOW 15 PROUFDE DETERMINE LIENT STILL REFRESH KEY REFRESH KEY AUTHOR IZED BASED ON TEME 550 540 ESTABLISH NO POINT-TO- POINT, VERTFY CREDENTIALS ADDITIONAL 6550 INTERVAL? YES 40 570 ENDE

FIG. T

FIG, 6



JHIL -INIT -> TEME EXTENIVE D FYLLIG PERFOU - FIRST THIERVAL NOT ENCRYPTED 200

P.E.

F161, 7

EGIN)

PECETUE AN INITIAL REQUEST FOR A KEY
FROM EACH OF A NUMBER OF CLIENTS AT
VARIOUS RAHDOM TIMES DURING A
PREDETERNINED PERSON REFORE THE EVENT

ESTABLISH POINT-10-POINT WITH EACH CLIENT G20

VERIFY CREDENTIALS

830

TRANSMIT INITIAL KEY 640

DETERMINE WHICK OF THE NUMBER
OF CLIENTS REMAIN AUTHORIZA FOR
A NEXT EVENT INTERVAL DURING
FORWARD SECURITY WINDOW 650

MULTICAST REFRESH LEY TO

CLIENTS THAT REMAIN AUTHORIZED

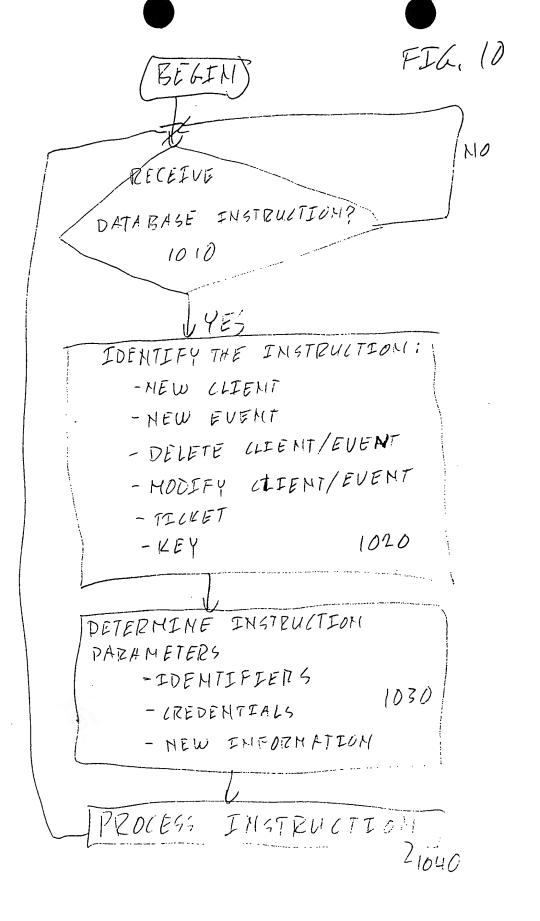
FOR NEXT INTERVAL 860

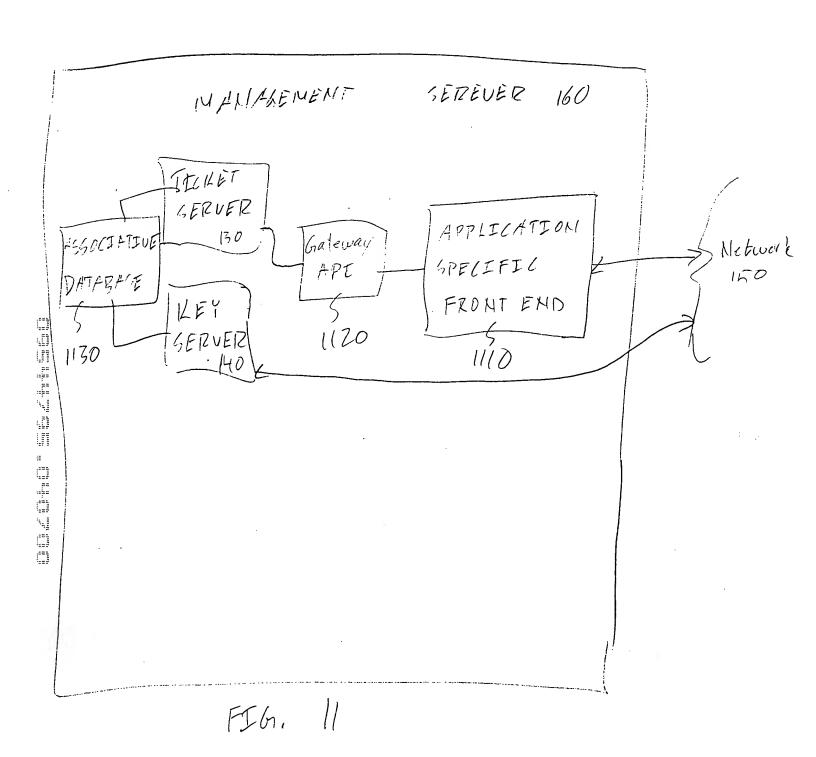
ADDITIONAL YES

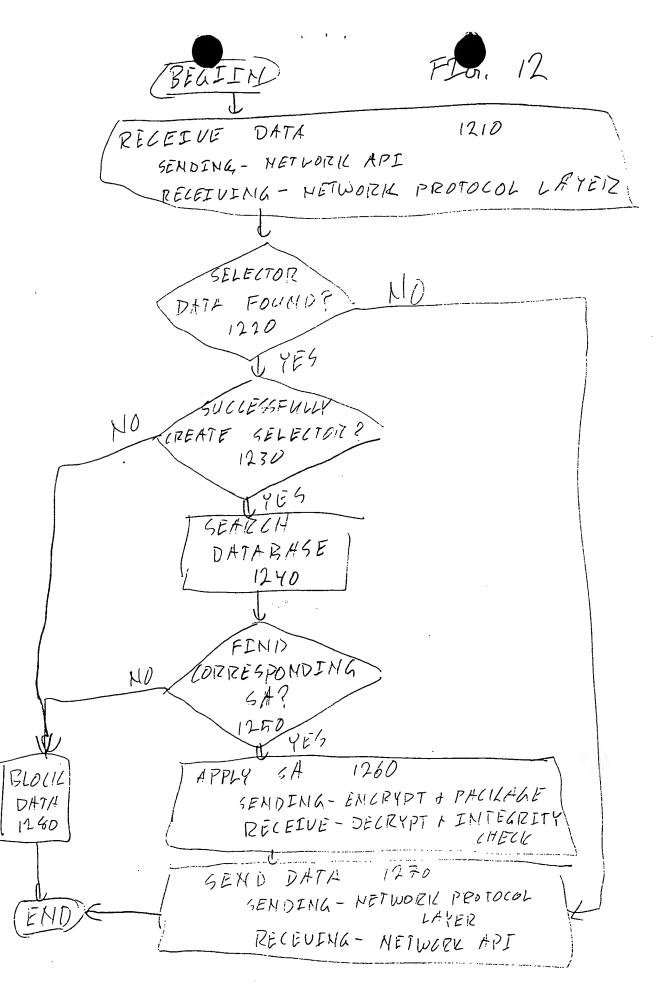
J11)

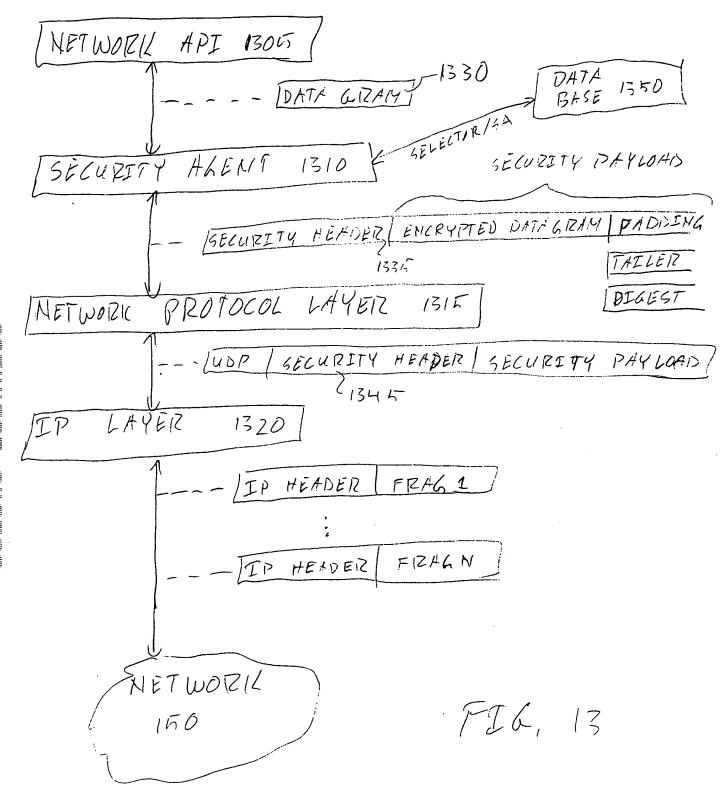
\$IG. 6

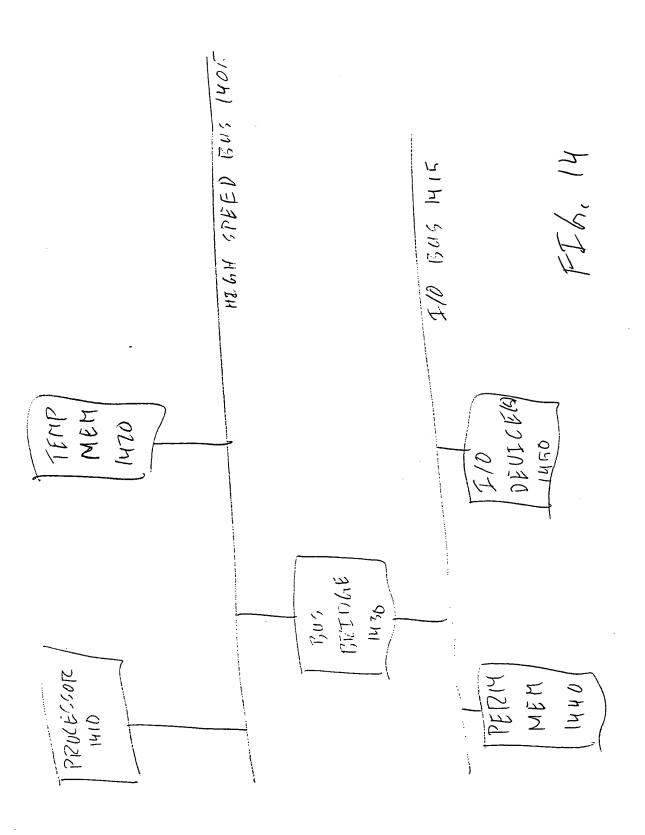
BEGIU) SEHD REQUEST TO TICKET GERVER 410 FIL. MECETUE TECKET FROM TECKET 920 GERVER IF AUTHORIZED TICKET INFO TO A USER 930/ PROUIDE RECEIVE EVENT SELECTION FROM USER BASED ON TICKET PROVIDENG A TITLE OF THE EVENT, AN IP APORESS OF SENDER, IP ADDRESS OF LEY SERVER, AND START TIME GENERATE RANDOM TIME DURING KNOWN 450 TO START TEME PERSOD\_ SEND REQUEST FOR KEY TO KEY SERVER FP ADDRESS AT THE RANCOU TIME, TERUEST FNCLUDING TITLE OF EVENT AND CREDENTIALS, THE REQUEST SUFFICIENTLY SYNCHRONIZED, 960 RECEIVE KEY - ENCRYPT KEY FOR SENDER, DECRYPT KEY FOR RECEIVED, TOLETHER COMPRILIENG SYMMETRIC 124PTOGRAPHIC KEY PARTICIPATE IN EVENT GGO! REFRESH KEYS AS LONG AS AUTHORIZED AND THERE ARE EVENT INTERVELS, EFFILE POINT - TO-POINT - GENERATE RANDON TEME FOR FIRST INTERVAL AND AT REGULAR INTERVALS THERE TIETS 000 OR MULTILAGE











MACHENE REFURBLE PIEDLUM 1520 NIACHTNE FXECUTABLE TAKTRUCTEONIS 1510

FIG. 15